AFRL-OSR-VA-TR-2014-0174

CYBERSECURITY LABORATORY

Leslie Guice
LOUISIANA TECH UNIVERSITY

08/01/2014
Final Report

Air Force Research Laboratory
AF Office Of Scientific Research (AFOSR)/ RTC
Arlington, Virginia 22203
Air Force Materiel Command

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
03 JUL 2014		**01-06-2009 to 31-05-2014**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Cybersecurity Laboratory	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Louisiana Tech University,Rail Road Ave,Wyly Tower 1620,Ruston,,LA, 71272**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**6**	

Cybersecurity Laboratory (Cyberspace Research Laboratory - CRL)

FA9550-09-1-0479

June 01, 2009-May 31, 2014

&

Cybersecurity Research Program at the CRL

FA9550-10-1-0289

July 1, 2010 – June 30, 2014

PI: Leslie K. Guice

Louisiana Tech University

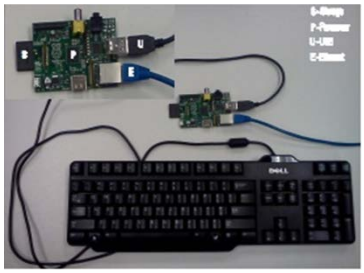
I. Highlights of the Accomplishments

(i) Developed a multi-faceted, unique Cyberspace Research Laboratory (CRL) at Louisiana Tech University to provide state of the art full-fledged support in cyber security research and experimentation.

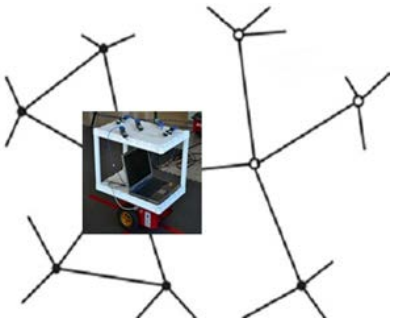
CRL consists of several unique facilities that include virtualization, visualization, networking, micro-aerial vehicle and sensor networks (MAVSeN), and FPGA laboratories. The Virtualization facility supports up to 400 virtual machines, is configurable to on-demand requirements, and can simulate various virtualized environments. The visualization facility offers the ability to render large and complex datasets and visualize them on a high resolution tiled display. The networking laboratory offers a variety of Cisco equipment for testing with different types of networks. The MAVSeN laboratory is equipped with MAVS with wireless sensor nodes, uses Vicon-based motion capture system as an indoor GPS-like navigation tool and includes gesture-based sensing and control.

(ii) Yielded several significant research outcomes with the support of the Cyberspace Research Laboratory.

A summary of the key accomplishments are presented below.

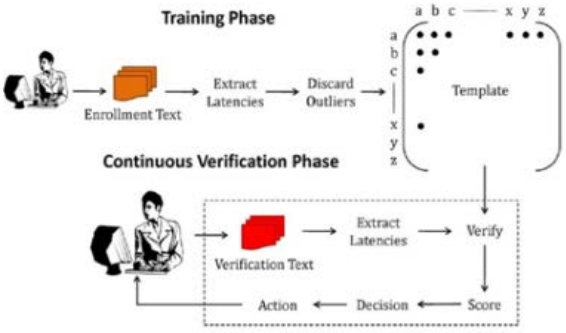


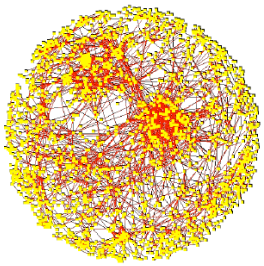
(a) **Developed the first non-interactive dual channel protocol for continuous authentication** that does not require users' explicit participation. A brief piece of information sent through a narrow band authenticated channel is used to authenticate information sent over a broad band insecure channel. Non-interactive nature of the protocol ensures that the protocol-communications are unidirectional and the work-load at the server end is not overwhelmed. Realized the protocol for an example application of preventing information exfiltration through continuous traffic authentication. Experiments with continuous traffic authentication show that, the 30 day daily average of false reject rate for all legitimate requests is 2.4% and the false accept rate for malicious traffic requests is 0% [1].



(b) **Developed algorithms for the navigation of Unmanned Ground Vehicles (UGVs) towards a set of pre-identified target nodes in coordinate-free and localization free wireless sensor and actuator networks** [2]. The UGVs are equipped with a set of wireless listeners that provide sensing information about the potential field generated by the network of actuators. Two main navigation scenarios are considered: single-UGV, single-destination navigation and multi-UGV, multi-destination navigation. For the single-UGV, single-destination case, we present both centralized and distributed navigation algorithms. Both algorithms share a similar two-phase concept. In the first phase, the system assigns level numbers to individual nodes based on their hop distance from the target nodes. In the second phase, the UGV uses the potential field created by the network of actuators to move towards the target nodes, requiring cooperation between triplets of actuator nodes and the UGV. The hop distance to the target nodes is used to control the main moving direction while the potential field, which can be measured by listeners on the UGV, is used to determine the UGV's movement. For the multi-UGV, multi-destination case, we present a decentralized allocation algorithm such that multiple UGVs avoid converging to the same destination. After each UGV determines its destination, the proposed navigation scheme is applied. The presented algorithms do not attempt to localize UGVs or sensor nodes and are therefore suitable for operating in GPS-free/denied environments.

(c) **Developed keystroke based spoof-resistant robust authentication solution with extensive analysis of possible attack vectors**. Two major attacks that we study include Snoop-Forge-Replay attacks that are launched using stolen keystroke timings [4] and statistical attacks that are designed using population statistics [3]. Both attacks are shown to have high success rates. Cognitive and demographic analysis of keystroke timings are used to defeat these attacks.





(d) **Developed a user interest based model and community extraction methodology using that model to identify ad hoc user communities** such as group of actors with shared malicious intent. Attained accuracy in community detection ranged between 70% to 98% for data obtained from CiteULike [5].

(e) **Developed randomized methodologies and techniques for reducing feature dimensionality of computer programs for faster detection of malicious applications.** Achieved as much as a 4% increase in prediction performance and a five-fold decrease in processing time [6].

II. Technology Transfers

- Keystroke based user identification solution has been transferred to US Air Force through industrial partner Assured Information Systems (AIS).
  Sponsor: AFRL

- Transition of keystroke based Active Authentication solution is underway through industrial partner Aegis Research Lab.
  Sponsor: DARPA

III. Publications

Journal Papers

[1] *Irakiza, D., Karim, M. E. and Phoha, V. V.*, "**A Non-Interactive Dual Channel Continuous Traffic Authentication Protocol**," IEEE Transactions on Information Forensics and Security(TIFS), Vol 9 (7), pp 1133-1140, July 2014

[2] *Zhang, G., Duncan, C., Kanno, J. and Selmic, R. R.*, "**Unmanned ground vehicle navigation in coordinate-free and localization-free wireless sensor and**

actuator networks," Journal of Intelligent and Robotic Systems, Springer, Volume 74, Issue 3-4, pp 869-891, June 2014

[3] *Serwadda, A., Phoha, V. V.*, "**Examining a Large Keystroke Biometrics Dataset for Statistical-Attack Openings**," ACM Transactions on Information and System Security (TISSEC), Volume 16 Issue 2, September 2013

[4] *Rahman, K., Balagani, K. and Phoha, V. V,*. "**Snoop-forge-replay Attacks on Continuous Verification with Keystrokes**," IEEE Transactions on Information Forensics and Security (TIFS), Vol. 8, Issue: 3, 528 – 541, March 2013

[5] *Nair V., Dua S.*, "**Folksonomy-Based Ad Hoc Community Detection in Online Social Network",** Social Network Analysis and Mining, December 2012, Volume 2, Issue 4, pp 305-328

[6] *Durand, J., Flores, J., Kraft, N., Smith, R. and Atkison, T.*, "**Using Executable Slicing to Improve Rogue Software Detection Algorithms**," International Journal of Secure Software Engineering, vol. 2, no. 2, 2011, pp. 53-64.

Selected Conference Papers

[7] *Gardner,A., Kanno,J., Selmic, R. R. and Duncan, C.,* "**Measuring Distance Between Unordered Sets of Different Sizes**," IEEE Computer Society Conference on Computer Vision and Pattern Recognition, *CVPR 2014,* Columbus, Ohio, June24-27, 2014

[8] *Ponomarev, S., Wallace, N. and Atkison, T.*, "**Detection of SSH Host Spoofing in Control Systems Through Network Telemetry Analysis**," *The 9th Cyber and Information Security Research Conference*, ORNL, Oak Ridge, TN, April 2014

[9] *Irakiza, D., Karim, M. E. and Phoha, V. V.*, "**A Non-Interactive Dual Channel Authentication Protocol for Assuring Pseudo-Confidentiality**," Network and Distributed System Security Symposium (NDSS) 2013 (short talk), San Diego, CA, Available: www.internetsociety.org/doc/non-interactive-dual-channel-authentication-protocol-assuring-psuedo-confidentiality, February, 2013

[10] *Ponomarev, S., Durand, J., Wallace, N. and Atkison, T.*, "**Evaluation of Random Projection for Malware Classification**," The 7th International Conference on Software Security and Reliability, Washington, DC, June 2013

[11] *Zhang, G., Selmic, R. R., Duncan, C. and Kanno, J.*, "**Multi-UGV Multi-Destination Navigation in Coordinate-Free and Localization-Free Wireless Sensor and Actuator Networks**," 52nd IEEE Conference on Decision and Control, December 10-13, 2013. Florence, Italy